University of Victoria

Records Management Policy

University Policy No: IM7700
Classification: Information Management
Approving Authority: Board of Governors
Effective date: June 2017
Supersedes: January 2010
Last editorial change:
Mandated review: June 2020

Associated Procedures:
Procedures for the Management of University Records
Procedures for the Access to and Correction of Information
Guidelines for the Secure Destruction and Deletion of University Records and Information

---

PURPOSE

1.00 The purpose of this policy is to:

- ensure that university Records are created, used, disposed of and preserved in a systematic manner, compliant with relevant legislation;
- ensure that Access is provided to Records in compliance with the *Freedom of Information and Protection of Privacy Act* (FIPPA); and
- define authorities, responsibilities, and accountabilities for Records Management.

DEFINITIONS

2.00 **Access** includes both disclosure of Records under FIPPA as a result of a request, and routine release of Records that contain information that is available to the public or to an individual.

3.00 **Administrative Authority** means individuals with administrative responsibility for Units including but not limited to: Vice-Presidents, Associate Vice-Presidents, Deans, Chairs, Directors, Executive Directors, Chief Information Officer, and other Unit heads.

4.00 **Disposition** means disposal of Records no longer needed for day-to-day operations by a Unit, through destruction, secure destruction, or transfer to the university archives.

5.00 **Records** means documents created or received, and retained in the day-to-day operations of business. These include, but are not limited to, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.

6.00 **Records Management** means the application of systematic control to the creation, use, maintenance, storage, retrieval, Disposition, and preservation of all forms of recorded information produced by the university in the conduct of its operations.

7.00 **Unit** means academic or administrative areas at the university, including but not limited to: faculties, departments, divisions, offices, schools and centres.

JURISDICTION/SCOPE

8.00 This policy applies to all Records in the custody or under the control of the university and to the management of Records by all Units.

POLICY

9.00 The university will manage Records in order to meet its business, fiscal, and legal requirements.

Roles and Responsibilities

10.00 Consistent with section 64(1) of the *University Act*, the University Secretary is responsible for the oversight of records management at the university.

11.00 The University Archivist is responsible for:

- maintenance of the university's Records Management program, including the university-wide Records classification, retention and Disposition plan;
- developing Records Management policy and procedures, and providing standards and guidelines to assist Units in the implementation of Records Management;
- providing Records Management training and advisory services to Units; and
- providing Access to university Records selected for permanent retention.

11.01 University Archives staff will assist Units with Records Management.

12.00 Administrative Authorities are responsible for making reasonable efforts to ensure that:

- Records in their Unit are managed according to this policy and related procedures;
- employees in their Unit manage Records according to this policy and related procedures;
- Records containing personal or confidential information are protected from unauthorized Access and disclosure, in accordance with the Protection of Privacy Policy (GV0235) and the Information Security Policy (IM7800) and related procedures.

13.00 When leaving a position, a university employee must ensure that university Records are left in the custody or under the control of the university.

14.00 The Coordinating Committee for Privacy, Records Management, and Personal Information Security has oversight on policies, procedures, strategies and guidelines needed to:

- establish and maintain a university-wide framework to manage university Records;
- meet the university's business, legal and fiscal requirements; and
- ensure preservation of the university's corporate memory through selecting Records for permanent retention.

15.00 Any Records that are in the custody or under the control of the university as a result of the terms of a contract must be managed according to this policy, the Protection of Privacy Policy (GV0235), and the Information Security Policy (IM7800).

Creation

16.00 Records are created by Units in order to carry out the university's business and perform necessary transactions. Units are expected to use the university-wide classification plan to classify Records, thereby enabling effective retention and Disposition.

Access

17.00 The university is committed to providing Access through routine release of Records where possible.

18.00 Access to Records not covered by routine release is governed by the university's Procedures for the Access to and Correction of Information.

Disposition

19.00 Records scheduled for Disposition containing personal or confidential information and identified as having no long-term value must be destroyed in a secure and permanent manner.

20.00 Records that will be kept permanently by the university will be held by and preserved for Access as determined by the University Archivist.

21.00 When the university retains an external organization to undertake work on its behalf, and that work involves the Disposition of Records, including those containing Personal Information, the university will enter into an agreement with that organization that requires the organization to return or destroy those Records in a secure and permanent manner.

22.00 Records scheduled for Disposition must not be Disposed of when such Records are:

- identified in current or pending litigation;
- responsive to a current request made under FIPPA;
- the subject of an audit; or
- identified in quasi-judicial and legal proceedings.

Authorities and Officers

i) Approving Authority: Board of Governors
ii) Designated Executive Officer: President
iii) Procedural Authorities: *Refer to individual procedures*
iv) Procedural Officers: *Refer to individual procedures*

Relevant Legislation

Freedom of Information and Protection of Privacy Act
University Act
Limitations Act

Related Policies and Documents

Associated Records Management Procedures

- Procedures for the Management of University Records
- Procedures for the Access to and Correction of Information

- Guidelines for the Secure Destruction and Deletion of University Records and Information Procedures for the Imaging of University Records

Protection of Privacy Policy (GV0235) and associated Procedures

- Procedures for the Disclosure of Personal Information in Emergency or Compelling Circumstances
- Procedures for the Management of University Surveillance Systems
- Procedures for Responding to a Privacy Incident or Privacy Breach
- Privacy Protection Schedule

Information Security Policy (IM7800)

University of Victoria

Procedures for the Management of University Records

Procedural Authority: University Secretary
Procedural Officer: University Archivist

Effective Date: June 2017
Supersedes: April 2015
Last Editorial Change: June 2013

Parent Policy: Records Management Policy (IM7700)

PURPOSE

1.00 The purposes of these procedures are to:

- assist Units in making reasonable efforts to create, use, maintain and dispose of university Records, whether in paper, electronic, audio-visual or other format, in a manner that:
  - complies with the *Freedom of Information and Protection of Privacy Act* (FIPPA) and other pertinent legislation; and
  - is consistent with the university's Records Management (IM7700), Protection of Privacy (GV0235) and Information Security (IM7800) policies and the Directory of Records;
- regulate the Disposition of university Records in all formats, whether paper, electronic or other; and
- describe the process for approving new or revising the existing functional classification structure, Series, and Retention Rules contained in the Directory of Records.

DEFINITIONS

2.00 The definitions contained in the university's Records Management policy (IM7700) apply to these procedures.

3.00 **Active Records** are Records that are maintained and used by a Unit or Units for current business.

4.00 **Authorized Disposition** means a Disposition of Inactive Records carried out with the approval of the University Archivist and the Unit's Administrative Authority (see also Disposition definition in IM7700).

5.00 **Directory of Records (DOR)** is the university-wide classification, retention and Disposition plan that arranges Records according to the functions of the university and identifies these functional groups by a block-numeric system for the efficient access, retrieval and Disposition of Records.

6.00 **Inactive Records** are Records that are no longer needed for current business.

7.00 **Primary Office** is an office or offices responsible for keeping the original and/or official versions of Records, and responsible for carrying out the approved Disposition of such Records.

8.00 **Retention Rules** are the instructions in the Directory of Records to Primary and Secondary Offices regarding the length of time for which records should be kept.

9.00 **Secondary Office** is an office or offices which may hold duplicate copies of university Records that are to be maintained for shorter retention periods than original and/or official versions of Records.

10.00 **Semi-active Records** are Records that are required infrequently for current business.

11.00 **Series** is a group of Records relating to a particular function, resulting from the same activity, or having a particular form. Within the Directory of Records functions, Records are arranged in Series.

12.00 **Transitory Records** are Records of temporary usefulness, required only for a limited period of time for the completion of a routine action or the preparation of an ongoing Record. Transitory Records do not include those Records required to meet statutory obligations, or to sustain administrative or operational functions. Transitory Records may include drafts, notes, calculations, and superseded documents.

13.00 **Vital Records** are Records that are necessary to re-establish or continue the business of the university in the event of a disaster, including those that are necessary to re-create the university's legal and financial position, necessary to preserve the rights of the university, its students and employees, and others associated with the university.

SCOPE

14.00 These procedures apply to all Units and to university Records held by external organizations that undertake work with the university.

PROCEDURES

Classifying and Managing Active and Semi-Active Records

15.00 Units should consult the Directory of Records in order to classify university Records for which they are responsible and identify the:

- function to which the file or single document relates;
- appropriate functional section from the Directory of Records (e.g., Financial Management, Human Resources, etc.);
- appropriate series by considering the action, content and source of the document; and
- primary and secondary number.

Units should consult university archives staff for Unit-specific advice on records classification.

16.00 Unit staff are expected to identify whether the Unit has any Vital Records and set procedures to give Vital Records the protection they require in case of disaster (the Directory of Records identifies Vital Records). The Primary Office, as identified on the Retention Rules, is responsible for ensuring the protection of Vital Records.

17.00 Unit staff are expected to identify the classification levels of the information and Records in the Unit for security purposes in accordance with the university's Information Security Classification Procedures.

18.00 Units should destroy or delete Transitory Records from files when such documents are no longer needed for reference.

18.01 Units should destroy or delete non-record materials when they are no longer required for reference by a Unit. Non-record materials include but are not limited to:

- published material such as books, pamphlets, circulars, newsletters, brochures, catalogues, and other information created for informational or reference purposes; and
- excess stock of forms.

Storage of Semi-Active Records

19.00 Units are responsible for storage of their own Semi-Active Records.

19.01 The university archives does not provide storage for Semi-Active Records.

Disposition of Inactive Records

20.00 Unit offices identified as Primary Offices for particular Record Series are responsible for conducting Authorized Dispositions of Inactive Records (whether in paper, electronic, audio-visual or other format) in accordance with the Directory of Records.

20.01 Units are responsible for determining on an annual basis what Records should be disposed of by consulting the Retention Rules of the Series that pertain to their activities.

- In consultation with Archives, use the Approved Retention Rule form for destruction of Records.

20.02 Some Series and sections in the Directory of Records have Retention Rules which are not yet approved. Incomplete retention rules do not preclude Authorized Disposition. In these cases, contact the University Archives for retention advice.

20.03 Refer to the university's Guidelines for the Secure Destruction and Deletion of University Records and Information for direction regarding acceptable forms of secure Records destruction. The method for Secure Destruction must be appropriate for the medium on which information is stored.

21.00 Unit offices not identified as Primary Offices for particular Record Series may destroy or delete such Records as specified for "other offices" in the approved Retention Rules, or when they are no longer useful to the Secondary Office. There is no requirement to conduct an Authorized Disposition.

Transfer of Records to University Archives

22.00 Records transferred to the university archives are deemed Inactive Records that are either:

- specified by the Retention Rules for transfer to the university archives; or
- identified as having long-term legal, administrative or historical value by the University Archivist (or designate), in consultation with the respective Unit staff.

23.00 When a Unit seeks to transfer Records to the University Archives, it must contact the:

- University Archives before sending any Records to ensure that only Records with archival value are transferred; and
- University Archivist directly if the Records intended for transfer are in electronic form only.

23.01 The University Archivist or Associate Archivist will provide further direction regarding the transfer of Records to the university archives.

Access to Records Transferred to the University Archives

24.00 Primary Offices may access their archival Records transferred to the university archives without restriction. Other offices may, on a need-to-know basis, access records on request to University Archives.

25.00 University Records transferred to the archives are arranged and described according to archival principles, are listed in publicly available databases, and are available for Access to the public unless Access is restricted by FIPPA.

Approval of changes to the Directory of Records

26.00 As a part of the ongoing management of university Records, the University Archivist will review the Directory of Records' functional classification structure, Series, and Retention Rules in light of changes to university functions, organizational structure, Unit responsibilities, technologies and relevant legislation.

27.00 Following consultation with the Privacy, Records Management and Personal Information Security Co-ordinating and Advisory Committees, Archives staff will work with Primary Offices to identify DOR sections for review.

28.00 Following agreement between Archives and Primary Office staff that the new or revised functional classification structure, Series, and Retention Rules reflect the required or desired changes, the draft revisions will be presented for approval to the Administrative Authority for the Primary Office.

28.01 If the draft revisions require further consultation, Archives and Primary Office staff will work together to incorporate desired changes.

29.00 Following approval of new or revised functional classification structure, Series, and Retention Rules by the Administrative Authority for the Primary Office, the draft changes will be presented to the DOR Sub-committee of the Privacy, Records Management and Personal Information Security Co-ordinating Committee for review.

29.01 If the DOR Sub-committee determines that the new or revised functional classification structure, Series, and Retention Rules presented need further revisions, Archives and Primary Office staff will work together to incorporate desired changes.

30.00 The DOR Sub-committee will provide summary notice of the recommended changes to the Co-ordinating Committee. After consideration of any comments from the Co-ordinating Committee, the University Archivist will recommend the new or revised functional classification structure, Series, and Retention Rules to the University Secretary for approval and signature.

31.00 Following the approval of the University Secretary, the relevant sections of the Directory of Records will be updated in the official version.

32.00 The official version of the Directory of Records is the on-line database.

33.00 The original approved and signed functional classification structure, Series, and Retention Rules will be kept in hard-copy in the University Archives.

34.00 Editorial changes to DOR that do not affect Records classifications or retention periods may be made upon written recommendation from the Administrative Authority for the Primary Office and the University Archivist to the University Secretary.

RELEVANT LEGISLATION

Freedom of Information and Protection of Privacy Act
Evidence Act (B.C.)
Federal and Provincial legislation pertinent to specific Units and Records

RELATED POLICIES AND DOCUMENTS

Protection of Privacy Policy
- Procedures for the Management of Personal Information

Records Management Policy
- Procedures for Access to and Correction of Information
- Guidelines for the Secure Destruction and Deletion of University Records and Information
- Procedures for the Imaging of University Records

Information Security Policy
- University Information Security Classification Procedures

Records Disposition Application – for records *without* an Approved Retention Rule
Records Disposition Application – for records *with* an Approved Retention Rule

University of Victoria

Procedures for Access to and Correction of Information

Procedural Authority: University Secretary
Procedural Officer: University Archivist

Effective Date: June 2017
Supersedes: January, 2010
Last Editorial Change: July, 2012

Parent Policy: Records Management Policy (IM7700)

PURPOSE

1.00 The purpose of these procedures is to set out how the university will manage:

- freedom of information requests;
- requests for correction of Personal Information in the university's custody or control;
- requests to access Records in the university archives;

in accordance with the *Freedom of Information and Protection of Privacy Act* (FIPPA), and where appropriate, the *Personal Information Protection Act*.

DEFINITIONS

2.00 The definitions contained within the university's Records Management (IM7700) and Protection of Privacy (GV0235) policies apply to these procedures.

PROCEDURES

RESPONDING TO REQUESTS FOR INFORMATION

Routine or Freedom of Information Access Requests

3.00 When an individual contacts a Unit seeking Access to his or her Personal Information or access to a Record in the custody or under the control of the university, the Unit's Administrative Authority (or designate) will assess whether the individual is seeking Access to:

(a) his or her Personal Information (e.g., the individual's file or a specific Record pertaining to that individual) only; or

(b) a university Record on a particular subject.

3.01 If the individual is seeking access to his or her Personal Information, after confirming the individual's identity, the Unit may disclose the information to the individual if that information can be disclosed routinely. This is considered a routine Access request.

3.02 If the Record(s) that the individual is seeking contains information about other individuals or was created with an expectation of confidentiality, the Unit will ask the individual to make a formal freedom of information request (FOI Access Request).

3.03 If the individual is seeking Access to university Records on a particular subject, the Unit may disclose the information to the individual if that information can be disclosed routinely. This is considered a routine Access request.

(a) If the Records contain information that the Unit believes is confidential (such that the information may be subject to exceptions in FIPPA), the Unit will ask the individual to make an FOI Access Request.

4.00 Routine access requests will be processed as quickly as possible.

Receiving a Freedom of Information Access Request

5.00 In accordance with FIPPA, FOI Access Requests must be made in writing. Units shall ask the individual to make a formal written request in one of the following ways:

(a) by completing and submitting the FOI Access Request form available on the University Secretary's website or in person at the University Secretary's Office; or

(b) by a written request that specifies the Records the individual is seeking.

5.01 Applicants must provide their full contact information.

5.02 The university may clarify an FOI Access Request.

6.00 If a FOI Access Request is for Records containing personal information, then the applicant must sign the request and provide proof of identity, which means government-issued photo identification matching the address and signature on the FOI Access Request.

6.01 If a FOI Access Request is for a third party's personal information, then the applicant must submit proof of consent by the third party, that complies with the FIPPA's regulations, and confirms the identity of the third party.

7.00 If a Unit receives an FOI Access Request, the Unit will forward it to the University Secretary's Office.

8.00 Records or information responsive to a request must not be destroyed after a request has been received.

9.00 Employees must treat, in a confidential manner, individuals' requests for Access to their own information and all FOI Access Requests. Information about access requests is to be used only to the extent necessary to respond to a request. Applicants shall not be asked the reason(s) for which they have requested the information or Record(s). If in doubt, employees should contact the University Secretary's Office.

Processing a Freedom of Information Access Request – Unit Responsibilities

10.00 Upon receiving an FOI Access Request, the University Secretary's Office will ask the Unit(s) to provide Records responsive to that request. Units are then responsible for following the applicable Reasonable Search Guidelines, including:

(a) Making one single-sided copy of the requested Records;
(b) Printing a single-sided copy of any electronic Records, including e-mails and attachments;
(c) Making arrangements with the University Secretary's Office for in-person pick up or delivery of materials while ensuring that security and confidentiality are maintained; and;
(d) Advising the University Secretary's Office of any other Unit(s) that may hold responsive Records.

11.00 If necessary, the Unit producing the Records will be contacted to answer any follow-up questions. The University Secretary's Office will handle all communication with the applicant.

12.00 FOI Access Requests must normally be processed within thirty (30) working days of their receipt, unless otherwise authorized by FIPPA and as determined by the University Secretary.

13.00 The university may consult with third parties in limited circumstances, in accordance with FIPPA, if Records contain information about such parties. The University Secretary's office will manage consultations with third parties subject to an FOI Access Request.

14.00 The university may charge fees for FOI Access Requests made for general information in accordance with FIPPA. No fees can be charged for FOI Access Requests for an individual's own information. In some cases, a Unit may be asked by the University Secretary's Office to estimate the number of hours (less an initial three hours) required to locate, retrieve and produce the Records, and provide an estimate of the number of responsive pages. The University Secretary's Office will inform the applicant of the fee estimate where applicable.

CORRECTION OF PERSONAL INFORMATION

15.00 An individual who believes there is an error or omission in his or her factual Personal Information in the custody or under the control of the university may request that the university correct that information.

16.00 When an individual contacts a Unit to request a correction to his or her personal information, Unit staff, as authorized by the Unit's Administrative Authority will assess if the individual is able to make the change through the university's online self-service portal. Personal Information that may be changed through the self-service portal includes: updates to phone numbers and addresses, additional e-mail addresses, and updates to emergency contact information.

(a) If the information cannot be changed by the individual through the online self-service portal, the Unit will inform the individual of the steps required to correct the factual personal information, including the provision of appropriate documentation.

17.00 If the steps set out in section 16.00 do not resolve the matter, the Unit will ask the individual to make his or her correction request by one of the following means:

(a) by completing and submitting the correction request form available on the University Secretary's website or in person at the University Secretary's office;
(b) by writing a letter that specifies the correction they are seeking, the location of the information (Unit responsible), a description of the information, the reasons for the correction and the individual's contact address; or
(c) by procedures established by the Registrar.

18.00 The university will process the request and determine if the correction will be made, and the University Secretary's Office or the Office of the Registrar will notify the individual in writing.

19.00 If the request is approved, the appropriate Unit will replace the information with the correct information in a timely manner.

20.00 If the request is denied, the appropriate Unit will annotate the information with the correction requested, in accordance with FIPPA.

21.00 Evaluative comments or assessments and opinions about individuals may, on request, be annotated but not corrected. Concerns regarding such information may be pursued through academic or Human Resources' channels.

22.00 If the University Secretary determines that a correction will be made to an individual's information, any other public body or any third-party to whom that information has been disclosed during the one year period before the correction was requested will be notified of the correction.

ACCESS TO RECORDS IN THE UNIVERSITY ARCHIVES

23.00 In accordance with FIPPA, the university archives may disclose Personal Information in university Records for archival or historical purposes.

23.01 Archival descriptions of university Records, also known as finding aids, will specify whether Records must be reviewed for any exceptions to disclosure under FIPPA prior to use of the Records.

24.00 The *Personal Information Protection Act* (PIPA) applies to records donated to the university archives by individuals and organizations and permits disclosure for archival or historical purposes.

The Associate Archivist or University Archivist will review records for Personal Information prior to Access by a person and apply PIPA including, if necessary, a research agreement regarding disclosure.

Archives Access Procedures

25.00 To access records in the university archives, an individual may contact the archives and identify the accession number and file titles of the Records that are required (located in the finding aid).

26.00 The University Archivist or Associate Archivist will review the file.

(a) If Records containing information that may be subject to any exceptions to disclosure under FIPPA can reasonably be removed from the file, the remainder of the file will be provided to the individual requesting access, as mutually agreed.

(b) If an individual requests Access to information that may be subject to any exceptions to disclosure under FIPPA, the University Archivist or Associate Archivist will ask the individual to make a FOI Access Request.

(c) If an individual requests Access to a large body of Personal Information that may be subject to any exceptions to disclosure under FIPPA, the University Archivist or Associate Archivist will discuss the use of a research agreement with the individual.

Research Agreements

27.00 Some university Records have Access restrictions. In accordance with FIPPA, the university may allow access to Records containing Personal Information for statistical and research use through the signing of a research agreement between the university and an applicant governing the conditions of Access and use.

RELEVANT LEGISLATION

Freedom of Information and Protection of Privacy Act
Personal Information Protection Act

RELATED POLICIES AND DOCUMENTS

Protection of Privacy Policy (GV0235)

- Procedures for the Management of Personal Information

Records Management Policy (IM7700)

- Procedures for the Management of University Records

Information Security Policy (IM7800)

- University Information Security Classification Procedures

Reasonable Search Guidelines (Records Containing Personal Information)
Reasonable Search Guidelines (Records Containing Non-Personal Information)

University of Victoria

Guidelines for the Secure Destruction and Deletion of University Records and Information

Procedural Authority: University Secretary, Vice-President Finance & Operations
Procedural Officers: University Archivist and Chief Information Officer

Effective Date: November 2014
Supersedes: July 2014
Last Editorial Change: June 2017

Parent Policies: Records Management Policy (IM7700)
Information Security Policy (IM7800)

PURPOSE

1.00 The purpose of these guidelines is to protect Records and information in the custody or under the control of the university from unauthorized use or disclosure by informing university employees of:

1.01 How to conduct the physical destruction of paper Records and electronic devices containing information that is classified as Internal, Confidential or Highly-Confidential under the university Information Security Classification procedures, or designated in the Directory of Records as requiring confidential destruction; and

1.02 How to conduct deletion of information in electronic form that is classified as Internal, Confidential or Highly-Confidential under the university Information Security Classification procedures, or designated in the Directory of Records as requiring confidential destruction.

DEFINITIONS

2.00 The definitions contained within the university's Records Management (IM7700) and Information Security (IM7800) policies apply to these procedures.

3.00 **Secure Destruction** means permanent physical destruction of paper records and electronic devices, rendering unreadable or unrecoverable the information they contain.

4.00 **Deletion** means removal of information from electronic devices and storage media.

4.01 **Routine Deletion** means removal or erasure of information from electronic devices and storage media by marking information as deleted. The information still exists, making data recovery possible unless the information is securely deleted or overwritten.

4.02 **Secure Deletion** means the process of deliberately, permanently, and irreversibly removing or erasing information from electronic devices and storage media.

5.00 Sanitization is a process to render access to target data (the data subject to the sanitization technique) on the device or media either effectively inaccessible (but potentially recoverable through data recovery techniques) or effectively irrecoverable. Deletion, erasure (deletion with overwriting), and destruction (physical destruction of the storage media) are actions that can be taken to sanitize media.

SCOPE

6.00 These guidelines apply to the following actions taken after the decision to dispose of Records and information consistent with Directory of Records (DOR) retention rules has been made:

6.01 The physical destruction of information, whether in paper, electronic, audio-visual or other format. This includes computers and other electronic devices and storage media (e.g. mobile phones); see section 16 below for further examples; and

6.02 The deletion of information in electronic form.

GUIDELINES

7.00 The method for Secure Destruction must be appropriate for the medium on which the information is stored.

Security Classification

8.00 Units are expected to refer to the security classification level of the information and Records prior to their destruction to assist in determining an appropriate destruction method. (See http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7800.pdf)

Authorization for Secure Destruction and Secure Deletion

9.00 Unit offices identified as Primary Offices for a particular Record series are responsible for obtaining authorization for Disposition from the University Archives prior to Secure Destruction or Secure Deletion in accordance with the university's Procedures for the Management of University Records and the Directory of Records. See http://www.uvic.ca/recordsmanagement/resources/forms/index.php for authorization forms.

9.01 Unit offices identified as Secondary Offices for a particular Record series may securely destroy or delete Records past their retention period without authorization from the University Archives.

Units are encouraged to consult the University Archives for specific guidance on Records Disposition, including Secure Destruction or Secure Deletion if they are not already familiar with the Disposition process.

Primary Office is an office or offices responsible for keeping the original and/or official versions of Records. Secondary Office is an office or offices which may hold duplicate copies of university Records that are to be maintained for shorter retention periods than original and/or official versions of Records.

Secure Destruction of Paper-Based Information

10.00 Records containing Highly-confidential, Confidential, and Internal information are to be shredded in a secure manner; Records containing public information may be recycled.

10.01 Records containing Highly-confidential information (see Information Security Procedures) should be shredded by a staff member of the Unit that holds the records, or on campus ("onsite") by an external supplier. Records containing Confidential or Internal information may be shredded off campus ("offsite") by an external supplier, or onsite by an external supplier or by a staff member of the Unit that holds the records.

Information Security Level	Highly-Confidential	Confidential	Internal	Public
Destruction, Paper Records	Onsite shredding	Offsite shredding (Onsite optional)	Offsite shredding (Onsite optional)	Recycle

11.00 Units should use the university's preferred external suppliers for shredding services. For supplier names, information on engaging them, and negotiated pricing, see https://www.uvic.ca/purchasing/resources/preferred-suppliers/index.php (requires NetLink logon).

11.01 If a Unit does not wish to use the preferred external suppliers for shredding services, the following conditions must be met:
- The external supplier must be NAID certified
- The service is selected in accordance with the Purchasing Services Policy (FM5105).

12.00 Units may consider the appropriateness of a Unit staff member supervising shredding by an external supplier, but this is not required.

13.00 Small quantities of paper Records may be shredded by individual Units. Contact Purchasing Services for recommended shredder models if necessary.
- If a Unit uses its own shredders, the Records must be shredded in a secure manner; secure methods include shredding into strips that are a maximum of one

centimetre wide, cross-cut shredding, re-shredding or mixing shredded Records to ensure that information cannot be reconstructed.

- For Records with Confidential or Highly-confidential information, cross-cut shredding or re-shredding is recommended.
- If such Records are not cross-cut shredded or re-shredded, the shredded Records should be mixed to ensure information cannot be reconstituted.

If a staff member of a Unit is uncertain about the security classification of the information or Record, the staff member shall use the destruction method for the higher level. Contact the Records Management Archivist with questions.

14.00 Records awaiting Secure Destruction must be kept in a secure manner (i.e. locked cabinet, controlled access area, secure supplier's console, or sealed boxes in a locked room).

Electronic Device or Storage Media Sanitization

15.00 The approach for handling electronic devices and storage media after use is dependent on whether the devices or media are being repurposed for university use or are no longer required for use.

Deletion of Electronic Device or Storage Media Information

16.00 Electronic devices and storage media purchased with university funds or funds administered through the university, and that are repurposed for university use, must have information Sanitized prior to being repurposed.

16.01 Electronic devices and storage media that will be repurposed for university use that contain information classified as Public or Internal may be Sanitized by Routinely Deleting all data on the device in a manner that renders it effectively inaccessible.

16.02 Electronic devices and storage media that will be repurposed for university use that contain information classified as Confidential or Highly-confidential must be Sanitized using a method that erases data by overwriting the data multiple times, prior to being repurposed to another Unit or employee. Erasing overwrites all addressable locations with a character, its complement, then a random character, and verifies. If you require assistance, contact the Computer Help Desk to arrange for erasing of devices and storage media.
http://www.uvic.ca/systems/services/contact/index.php

16.03 For best practices on Deletion and erasure, please see the "How To" section on the following University Systems service page:
http://www.uvic.ca/systems/services/informationsecurity/diskencryption/index.php

Destruction of Electronic Devices or Storage Media

17.00 Electronic devices and storage media purchased with university funds or funds administered through the university, that are not repurposed for university use, must undergo secure physical destruction when no longer required by a Unit or employee, whether or not they are known to store Internal, Confidential, or Highly-confidential information.

17.01 Units must use the central secure physical destruction program provided by University Systems and Purchasing Services. Contact the Computer Help Desk to arrange for Secure Destruction of electronic devices and storage media. http://www.uvic.ca/systems/services/contact/index.php

17.02 Electronic devices and media requiring secure physical destruction include, but are not limited to: hard drives, flash media, USB keys, thumb drives, CDs, DVDs, floppy disks, computer tapes, audio and video storage devices, PDAs, Smart Phones and cell phones, and hard drives in all printers and copiers.

RELATED POLICIES AND DOCUMENTS

Protection of Privacy Policy (GV0235)

- Procedures for Responding to Privacy Incidents or Privacy Breach

Records Management Policy (IM7700)

- Procedures for Access to and Correction of Information
- Procedures for the Management of University Records
- Procedures for the Imaging of University Records

Information Security Policy (IM7800)

- University Information Security Classification Procedures
- Procedures for Responding to an Information Security Breach

RESPONSIBLE OFFICES

Information Security Office
University Archives